IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

IN RE: DEALER MANAGEMENT SYSTEMS ANTITRUST LITIGATION	MDL No. 2817 Case No. 18-cv-00864
This Document Relates To: *Authenticom, Inc. v. CDK Global, LLC, et al.*, Case No. 1:18-cv-00868 (N.D. Ill.)	Hon. Robert M. Dow, Jr. Magistrate Judge Jeffrey T. Gilbert **PUBLIC-REDACTED**

PLAINTIFF AUTHENTICOM, INC.'S STATEMENT OF UNDISPUTED MATERIAL FACTS IN SUPPORT OF ITS MOTION FOR SUMMARY JUDGMENT ON DEFENDANTS' COUNTERCLAIMS

Plaintiff Authenticom, Inc., pursuant to Federal Rule of Civil Procedure 56 and Northern District of Illinois Local Rule 56.1, hereby file their Statement of Undisputed Material Facts in Support of Its Motion for Summary Judgment On Defendants' Counterclaims.

STATEMENT OF UNDISPUTED MATERIAL FACTS

1. Dealer Management System ("DMS") software is enterprise software that franchised automobile dealerships rely on to manage their operations. Ex. 150, Expert Report of Allan Stejskal ("Stejskal Rep.") ¶ 24; Ex. 90, PX 1383 at REYMDL00016579 ¶ 2; Ex. 4, Declaration of Brian Maas, President of the California New Car Dealers Association ("Maas Decl.") ¶ 4, *Authenticom* Dkt. 56 (DMS "software is mission-critical software that every dealership relies on to manage and direct its operation" and store its data); Ex. 57, DX 230, FTC Auto/Mate Complaint (March 19, 2018) ("FTC Auto/Mate Complaint") ¶ 24 ("The DMS is a mission-critical business software that serves as the backbone of the dealer's information technology systems.").

2. The DMS includes a database that stores data central to dealership operations, such as information related to customers, service appointments, and car and parts inventory. Ex. 150, Stejskal Rep. ¶ 30 ("At the heart of the DMS is a database that stores dealer data, which supports all of the various functions performed at a dealership."); [redacted] Ex. 3, Declaration of Chris Longpre, Owner and Vice President of Lexus of Westminster car dealership ("Longpre Decl.") ¶ 4, *Authenticom* Dkt. 55 ("The DMS contract is a significant expense for . . . dealers[ ]. As part of the contract, we pay CDK to store our dealership data. That data includes vehicle, inventory, customer, sales, and other of our most important information. CDK does not own that data. We do."); [redacted]

[redacted]

3. Dealers input data they generate in their day-to-day operations into the DMS database. [redacted]

Ex. 6, Declaration of Leigh Ann Conver ("Conver Decl.") ¶ 10, *Authenticom* Dkt. 90 ("CDK's DMSs hold, among other information, the dealer's operational and business data."); Ex. 1, Declaration of Wayne Fitkin, IT Director for Walter's Automotive Group ("Fitkin Decl.") ¶ 4, *Authenticom* Dkt. 53 ("As part of the contract, we pay CDK to store data owned by Walter's Automotive Group. Walter's Automotive Group owns the data that is on its DMS system.").

4. CDK has long stated that dealers "own" – that is, control – the data they store on the DMS database. Ex. 95, PX 1726 at CDK-3122863 (CDK CEO Mr. Anenen stating: "[A] dealership fundamentally owns the data in its DMS, and dealers should control who accesses their data and how it's used."); Ex. 66, PX 228 at CDK-0804051 (Kevin Henahan, ADP's Senior Vice President for Marketing, stated: "First, it's the dealer's data. . . . We do a lot of things to provide security for the dealer systems and their data."); Ex. 130, CDK-3122449 (2008 CDK "NewsFlash" stating "[o]ur view is that it is the dealers data to share with other companies as they see fit, as long as they acknowledge the risks"); *id.* at 450 ("ADP has always understood that dealerships own their data and enjoy having choices on how best to share and utilize that data with others."); Ex. 108, CDK-0043287 (April 27, 2016) (Mark Hnilicka, CDK's Vice President and General Manager for Enterprise Accounts, stating: "Do not get me wrong – I am all for security – but we have ALWAYS told the dealer their data was theirs – not ours"): [redacted]

[redacted]

Ex. 150, Stejskal Rep. ¶¶ 59-60.

5. Reynolds has repeatedly acknowledged that dealers own the data they store on the DMS database. Ex. 73, PX 636 (Reynolds advertisement stating: "You own your data and choose who you allow access to it."). Ex. 74, PX 637 (Reynolds webpage stating: "You own your data."); [redacted] Ex. 150, Stejskal Rep. ¶¶ 59-60.

6. In 2018, there were 16,794 franchised new car dealership locations – called "rooftops" – in the United States. Ex. 151, Expert Report of Mark Israel ("Israel Rep."), ¶ 15 (citing National Automobile Dealers Association figures).

7. CDK and Reynolds have a combined market share of at least 70 percent in the market for DMS services with respect to franchised, new-car dealerships in the United States, when market share is measured by dealership rooftop (i.e., franchised stores). [redacted] Ex. 57, DX 230, FTC Auto/Mate Complaint ¶ 31 ("The U.S. Franchise DMS Market is highly concentrated, with CDK and Reynolds controlling roughly 70% of the market."); [redacted]

8. [redacted] Ex. 150, Stejskal Rep. ¶ 39 ("Large dealership groups (those with multiple rooftops) in particular work almost exclusively with CDK and Reynolds.").

9. In addition to the DMS, dealers use other software applications to help them sell and service cars. *See* Ex. 163, CDK Global, *Is the Cheaper DMS Really Better?* (May 3, 2017) ("A DMS can't stand alone. It needs to work seamlessly with F&I, Parts & Service, Sales, Accounting and even OEM integrations."), https://www.cdkglobal.com/us/insights/cheaper-dms-really-better; Ex. 58, DX 405 at COX_0020334 ¶ 7 (there are "various third party application tools that dealers will use to supplement the functionality of their franchise dealer DMS"); Ex. 6, Conver Decl. ¶ 11, *Authenticom* Dkt. 90 ("Many dealers contract with third-party providers ('vendors') that offer software applications that perform operational functions for dealerships.").

10. Commonly used applications include vehicle inventory management, customer relationship management ("CRM"), electronic vehicle registration and titling ("EVR"), service and repair appointment scheduling, and lead generation and marketing. Ex. 150, Stejskal Rep. ¶ 49 (describing popular application types); Ex. 7, Declaration of Howard Gardner ("Gardner Decl.") ¶ 3, *Authenticom* Dkt. 93 (same).

11. To function, third-party applications often depend on access to the dealer's data stored on the DMS database. Ex. 6, Conver Decl. ¶ 11, *Authenticom* Dkt. 90 ("As a general matter, in order to provide these services, the vendors must have access to a dealer's data."); [redacted] Ex. 150, Stejskal Rep. ¶ 55 ("Each of these applications is reliant on a core set of data that powers the application.").

12. Historically, companies called data integrators have provided services that facilitate third-party application access to data stored on a dealer's DMS. Ex. 5, Declaration of Steve Cottrell ("Cottrell Decl.") ¶ 7, *Authenticom* Dkt. 62 ("[S]eparate companies – called 'data integrators' – specialize in extracting dealers' data from their DMS databases, organizing it, and delivering to vendors the specific data required for their applications."). Ex. 150, Stejskal Rep. ¶ 61 ("There is a long history of companies that have provided data integration services to dealers and to software vendors seeking the use of dealer data in order provide services to the dealers.").

13. Data integrators provide a variety of services that convert the dealer's data into a format that is easy for dealers and vendors to use. Ex. 5, Cottrell Decl. ¶ 9, *Authenticom* Dkt. 62 (data integrators provide "automated, seamless [data integration] without the need for manual intervention by dealers"; convert data "from a raw, unorganized state into a standardized format that is easy for vendors to use"; "correct data-entry errors or anomalies"; and standardize data from various DMS databases into a single format); Ex. 150, Stejskal Rep. ¶¶ 62-65 (describing range of services provided by data integrators).

14. CDK acquired two data integrators – Digital Motorworks ("DMI") in 2002 and IntegraLink in 2010 – through which CDK provides data integration services on several different DMS types, including CDK and Reynolds. Ex. 7, Gardner Decl. ¶¶ 75-77, *Authenticom* Dkt. 93;

Ex. 150, Stejskal Rep. ¶ 66 ("CDK saw sufficient value in the services provided by third-party integrators to acquire both DMI (in 2002) and IntegraLink (in 2010) in order to provide these integration services across all DMS providers.").

15. Dealers authorize data integrators to access their data stored on the DMS. [redacted] Ex. 1, Fitkin Decl. ¶ 9, *Authenticom* Dkt. 53 ("Walter's Automotive Group specifically authorizes Authenticom to pull our data from the DMS."); [redacted]

16. Dealers may create separate login credentials unique to data integrators to access the DMS database. [redacted] Ex. 6, Conver Decl. ¶ 11, *Authenticom* Dkt. 90 ("Dealers often provide or create login credentials for third party intermediaries, like Authenticom, who access the DMS on behalf of vendors without the DMS provider's authorization."); Ex. 7, Gardner Decl. ¶ 30, *Authenticom* Dkt. 93 ("Dealers have facilitated data access . . . by providing or creating login credentials for them to access the DMS"); [redacted] Ex. 150, Stejskal Rep. ¶ 68 (describing "[u]ser emulation" method of access in which "the dealer provides a User ID and password with the appropriate security

privileges to a third-party data integrator or application provider," which can "then execute functions that might run a report or create or update particular data in the DMS.").

17. The CDK DMS gives dealers the ability to create additional user accounts and to specify the permissions for those accounts. [redacted]; Ex. 9, Supplemental Declaration of Wayne Fitkin ("Fitkin Reply Decl.") ¶ 7, *Authenticom* Dkt. 141 ("The process I use to create this user ID and password [for Authenticom] is essentially the same way I grant access to new employees of the dealership. I note that CDK does not require me to provide the identity of or background information about the employees who will be granted access to the dealer's DMS. I am allowed to make those decisions myself, just as I should be allowed to choose which agents of the dealership are allowed to pull dealer data.").

18. The Reynolds DMS gives dealers the ability to create additional user accounts and to specify the permissions for those accounts. [redacted]

19. Authenticom was founded in 2002 by the entrepreneur Steve Cottrell, who at first ran the business out of a room in his son's apartment. Ex. 5, Cottrell Decl. ¶ 1, *Authenticom* Dkt. 62; Ex. 13, PI Hearing Tr. 1-A-88 to 1-A-89 (Q: "How many employees did it start with?" A: "One." Q: "So from those beginnings, could you please describe the growth of your business? A: "Essentially started in my son's bedroom, as the President stated.").

20. By 2015, Authenticom grew to 120 employees based in La Crosse, Wisconsin. Ex. 5, Cottrell Decl. ¶ 2, *Authenticom* Dkt. 62.

21. In a July 2, 2015 speech in La Crosse, Wisconsin, President Barack Obama heralded Authenticom as "one of America's fastest growing private companies" and noted Authenticom provides its employees with well-paying jobs and an equity stake in the company's

success. President Obama's speech is available at www.youtube.com/watch?v=Bfzu9kd5HU8. Ex. 5, Cottrell Decl. ¶ 74, *Authenticom* Dkt. 62.

22. At its height in early 2015, Authenticom provided data integration services to nearly 500 software vendors at 15,000 dealer rooftop locations. Ex. 5, Cottrell Decl. ¶ 34, *Authenticom* Dkt. 62.

23. Authenticom only accesses dealer data with the dealer's express, written authorization. Ex. 5, Cottrell Decl. ¶ 24, *Authenticom* Dkt. 62 ("Before Authenticom pulls data from a dealership, it gets specific authorization from the dealer."); Ex. 2, Declaration of Michael Korp ("Korp. Decl.") ¶ 25, *Authenticom* Dkt. 54 ("Several of our vendors use Authenticom to pull the dealerships data. I have expressly and specifically authorized Authenticom to perform this service."); Ex. 1, Fitkin Decl. ¶ 9, *Authenticom* Dkt. 53 ("Walter's Automotive Group specifically authorizes Authenticom to pull our data from the DMS."); [redacted]

24. Dealers create login credentials for Authenticom to access the DMS database. Ex. 5, Cottrell Decl. ¶ 24, *Authenticom* Dkt. 62 ("Dealers set up separate login credentials for Authenticom so that Authenticom can access the DMS database."); [redacted]

25. After the dealer creates login credentials for Authenticom, the dealer can revoke those credentials at any time. Ex. 164, Declaration of Steve Cottrell (May 19, 2020) ("Cottrell

5/19/20 Decl.") ¶ 4 (After dealers set up login credentials for Authenticom to access the DMS database, "[d]ealers can revoke the login credentials . . . at any time." Once a dealer de-activates Authenticom's login credentials, "Authenticom's access to the dealer's DMS database is shut off and Authenticom has no ability to access the DMS.").

26. Dealers control the data to which Authenticom has access through their ability to control the permissions associated with the credentials given to Authenticom. Ex. 164, Cottrell 5/19/20 Decl. ¶ 5 ("Dealers control the permissions associated with Authenticom's login credentials."); Ex. 14, PI Hearing Tr. 2-A-8:1-9:21 (Fitkin Testimony) ("What I have done for Authenticom is create a user ID just for Autenticom that has access to a single function" to perform user emulation . . . "Authenticom has access to limited accounts and to a single function . . . for the purpose of retrieving the data that I need them to retrieve so that they can – I like to call it feeding the children. All the third-party vendors that need the data, I call that feeding the children. So they gather the data, normalize the data, check the addresses against the NCOA database, and then send the feeds to a couple dozen third-party vendors that I use.").

27. Authenticom accesses the DMS in the same way that a dealer employee would; Authenticom's software "emulates" a dealer employee's use of the DMS, allowing for automated extraction of or writing of data to the DMS. Ex. 5, Cottrell Decl. ¶ 25, *Authenticom* Dkt. 62 ("Once dealers set up login credentials for Authenticom, Authenticom automates the pulling of data through user emulation software, which uses the DMS application software to run and capture reports in the same way a user at a dealership would. The difference is that integrators like Authenticom automate the process, whereas a user at the dealership would retrieve the data manually."); Ex. 13, PI Hearing Tr. 1-A-108:15-19 ("Essentially what we do is through terminal emulation or keyboard emulation, we utilize the application layer of the DMS system just like an

employee would. Essentially we're an employee at the dealership typing in the data request only we have very fast fingers."); Ex. 24, Clements Tr. 97:1-5 ("We would – with the authorization of the dealer, we would utilize their version of the software to pull the data for them in an automated fashion just as if they were standing in front of the dealer themselves."); Ex. 9, Fitkin Reply Decl. ¶ 6, *Authenticom* Dkt. 141 (Authenticom "pull[s] the exact same data that I could myself (or one of my employees could) pull.").

28. Authenticom employees did not believe their access of Reynolds's and CDK's DMS was unauthorized or prohibited by contract. Ex. 44, Cottrell Tr. 10:17-11:2 (Q: "Did there come a time when you understood that CDK objected to your polling data from the CDK system?" A: "Actually, no. Because our position was that we were polling data for the dealers at the dealers' authorization acting as their agent."); *id.* at 22:13-17 ("Our authorization came from our relationship with the dealers. The dealers paid, you know, lots and lots of money for access to that system. And we were authorized by the dealers, you know, to pull that data."); Ex. 24, Clements Tr. 260:11-13 ("We were dealer agents based on your dealer authorization, which allowed us to collect the data on their behalf."); Ex. 45, Brown Tr. 244:4-6 ("Additionally, we had authorization from the dealers to act as their agent to pull the dealers' data."); Ex. 37, Noth Tr. 69:22-70:4 ("[W]e get authorization from the dealers . . . to access the systems as their agent.").

29. In the fall of 2013, Authenticom released its DealerVault data integration platform. Ex. 97, AUTH_00148142 (September 5, 2013) (press release announces the launch of DealerVault, "the first ever cloud-based system that allows dealerships to control the distribution of their data."); Ex. 96, AUTH_00123382 (November 5, 2013) (DealerVault "getting [its] first dealers on-boarded."); Ex. 37, Noth Tr. 184:22-185:3 (discussing pricing for DealerVault in October 2013).

30. DealerVault offered a dealer-controlled data integration product. Ex. 11, PI Hearing Tr. 1-P-183:14-184:7 (California New Car Dealers Association President Brian Maas testifying regarding DealerVault: "I think it's the best product in its market space. There's no user interface that's easier to use. The fact that it limits by field, et cetera, as we saw in the demonstration this morning, all the feedback that we've heard from our dealer members it's a quality product."); Ex. 13, PI Hearing Tr. 1-A-90:21-25 (Mr. Cottrell testifying: "There's a tremendous need in the marketplace for dealers to be able to take control, have visibility, transparency, and control of their data. Not only did we see an opportunity in the market, but we saw a tremendous need and really felt that this was something we could do for the industry.").

31. Authenticom's enters into contracts with dealers who use DealerVault called the DealerVault Terms & Conditions. *See* Ex. 104, CDK-0012573.

32. The DealerVault Terms & Conditions provide that "DealerVault shall only extract the Dealership Data that the Dealership permits DealerVault to extract." Ex. 104, CDK-0012573 § 3.4.

33. DealerVault gives dealers "complete and total control" over how their data is distributed to the dealer's software vendors. Ex. 10, Reply Declaration of Steve Cottrell ("Cottrell Reply Decl.") ¶ 14, *Authenticom* Dkt. 143; Ex. 44, Cottrell Tr. 30:19-31:2 ("DealerVault provides a platform for dealers to syndicate their data with complete transparency and control to vendors of their choice.").

34. DealerVault provides an interface where dealers can add, remove, or change the specific data fields that Authenticom sends to specific vendors on the dealer's behalf. Ex. 5, Cottrell Decl. ¶ 29, *Authenticom* Dkt. 62 ("DealerVault provides a unified user interface where dealers are able to add, remove, or change the data sets that Authenticom sends to the vendors on

the dealer's behalf."); Ex. 13, PI Hearing Tr. 1-A-90:14-18 (Mr. Cottrell testifying: "DealerVault is a front-end web-based application that allows dealers complete control over their data. It allows them to see with full transparency and deliver data to their vendors of their choosing and control the access to that data to a granular level."); Ex. 45, Brown Tr. 219:14-18 ("But we only work with vendors that have specific authorization from a dealer. So if a dealer was to, you know, shut down their business with a vendor, we would then shut down the vendor."); Ex. 164, Cottrell 5/19/20 Decl. ¶ 8.

35. When dealers use Authenticom's services, they control the categories of data which Authenticom accesses. Ex. 164, Cottrell 5/19/20 Decl. ¶ 7 ("Dealers control the categories of data in the DMS database that Authenticom accesses. For example, dealers can choose to have Authenticom access to inventory data but not sales data"); Ex. 45, Brown Tr. 179:6-8 ("We only pull the fields – well, we only pull the fields and the elements that the dealer authorizes us to pull."); Ex. 10, Cottrell Reply Decl. ¶ 13, *Authenticom* Dkt. 143 ("As a matter of practice, Authenticom requests access from the dealers to retrieve data from the five aforementioned directories. Authenticom does not access any data beyond those five directories unless specifically directed to do so by a dealer Authenticom is thus limited to accessing data in the DMS that is controlled by the dealers.").

36. Through the DealerVault user interface, dealers control the frequency with which their data is distributed to their vendors. Ex. 164, Cottrell 5/19/20 Decl. ¶ 9 ("Through the DealerVault online portal, dealers control the frequency with which Authenticom distributes the dealer's data to vendors. For example, dealers can choose to have Authenticom provide data integration services at multiple intervals during the day, once at night, once a week, or even once a month depending on the dealer's needs for a particular vendor. Dealers can set the frequency of

data integration on a vendor-by-vendor basis, so that some vendors receive data more frequently and others less frequently"); Ex. 45, Brown Tr. 134:16-135:4 ("Now, the data is – once we have it in DealerVault, and if a dealer has chosen a specific vendor, then the frequency by which we send the data is up to the program or the necessity of the vendor . . . ." Q: "Does the dealer have the ability to determine or change that frequency?" A: "Yes, of course.").

37. DealerVault allows dealers to review records of the data sent to or received from software vendors. Ex. 13, PI Hearing Tr. 1-A-90:18-19 (Mr. Cottrell testifying that DealerVault provides "audit and reporting capabilities for the data that's been transmitted"); [redacted]

38. DealerVault gives dealers transparency about the software vendors that receive the dealer's data through the DealerVault service. Ex. 11, PI Hearing Tr. 1-P-134:23-135:1 (Defendants' security expert, Eric Rosenbach testifying: "[W]hen we talk about transparency, DealerVault itself, I think, is good. That's an impressive piece of technology. It does give the dealer transparency on data that's there and where it's going."); Ex. 12, PI Hearing Tr. 2-P-168:20-169:2 (CDK executive Howard Gardner testifying that it is "implausible" that dealers using "Authenticom's DealerVault" do not "know where [their] data is going").

39. Dealership principals and executives have lauded the control that DealerVault provides them over their data. Ex. 14, PI Hearing Tr. 2-A-6:11-7:15 ("I think it's an incredibly exceptional product when it was first offered to me when I worked for Fletcher [a dealership group]. I signed all 20 of our franchises up for it. It's the best thing I have ever seen because for once I had a single pane of glass to see every third-party vendor that was receiving data."); Ex. 1,

Fitkin Decl. ¶ 6, *Authenticom* Dkt. 53 ("Walter's Automotive Group has been using Authenticom's DealerVault product for the past year. I am extremely satisfied with this product, as it allows me to view and control exactly what data is being transmitted to third-party application providers."); Ex. 9, Fitkin Reply Decl. ¶ 7, *Authenticom* Dkt. 141 ("One major benefit of using Authenticom's DealerVault product is that it allows me to select, and thus limit, the particular types of data that I can send to a given vendor."); Ex. 3, Longpre Decl. ¶ 10, *Authenticom* Dkt. 55 ("If I had my choice, I would use Authenticom's DealerVault service for all of my vendors. DealerVault is more cost effective and provides dealers with a secure system and substantial control over their data, which CDK does not offer.");

40.

[redacted]

41. Brian Maas, the President of the California New Car Dealers Association, stated in a sworn declaration: "For those dealers that use or wish to use Authenticom's DealerVault product it is important that it gives them complete control and visibility over how their data is extracted and distributed to application providers." Ex. 4, Maas Decl. ¶ 15, *Authenticom* Dkt. 56.

42. Dealers consider Authenticom to be their agent when Authenticom provides data integration services on the dealer's behalf. [redacted] Ex. 11, PI Hearing Tr. 1-P-196:24-197:1 (Michael Korp, Ghaben Auto Group) (Q: "When Authenticom pulls your data, do they act as your agent?" A: "Yes."); Ex. 9, Fitkin Reply Decl. ¶ 8, *Authenticom* Dkt. 141 ("Dealerships contract with Authenticom to provide integration services for the dealers, and dealerships expressly authorize Authenticom to act as an agent on their behalf to provide data integration services that I could also provide in-house.").

43. [redacted]

[redacted]

44. [redacted]

45. [redacted]

[redacted]

46. CDK's DMI and IntegraLink data integration service providers have relied on login credentials created and provided by dealers, in order to provide data integration services. [redacted] Ex. 1, Fitkin Decl. ¶ 9, *Authenticom* Dkt. 53 ("Walter's Automotive Group has authorized other data aggregators, including Digital Motorworks and IntegraLink (both owned by CDK), to pull data in this exact same way – i.e., we provided a username and password to CDK's subsidiaries so they could pull the data just as Authenticom does.").

47. CDK's DMI and IntegraLink data integration service providers both used "user emulation" to access dealer data. [redacted]

[redacted]

48. [redacted]

[redacted]

49. [redacted]

[redacted]

50. [redacted]

[redacted]

51. [redacted]

[redacted]

[redacted]

52. [redacted]

[redacted]

[redacted]

53. CDK uses standard form contracts called the Master Services Agreement ("MSA") for providing its DMS to dealers. [redacted]

54. Since at least 2008, CDK's standard MSA has granted the "Client" – the dealer – a license to use the DMS. [redacted]

55. Since at least 2008, CDK's standard MSA has allowed the "Client" to "make available" the "CDK Products" – which includes the DMS – and any associated "screen displays" to the "Client's" "employees and agents" but not to "third parties." [redacted]

56. [redacted]

57. [redacted]

58. [redacted]

59. [redacted]

60. [redacted] Ex. 9, Fitkin Reply Decl. ¶ 14, *Authenticom* Dkt. 141 (Walter's Automotive Group noting NSA that allowed it to "provide a third party vendor with a user id and password into the Client's CDK DMS System to allow routine screen scrape of the DMS"); [redacted]

61. Reynolds enters into standard contracts with dealers called the Reynolds Master Agreement, the Reynolds Defined Terms, and the Reynolds Customer Guide. [redacted]

62. [redacted]

63. [redacted]

64. [redacted]

65. [redacted]

66. [redacted]

67. Since approximately 2006, Reynolds has publicly criticized the use of third-party data integrators. Ex. 5, Cottrell Decl. ¶¶ 35-36, *Authenticom* Dkt. 62.

68. Reynolds provides a data integration service – called the Reynolds Certified Interface ("RCI") program – for vendors to use to access data stored on Reynolds's DMS. [redacted]

69. Reynolds has engaged in extensive "whitelisting," which is Reynolds's practice of granting exemptions so that login credentials used by data integrators are not impeded by Reynolds's technological blocking (so-called "security") measures. [redacted]

70. [redacted]

71.

72. For many years, CDK supported the dealer's right to use data integrators. Ex. 131, CDK-3122862 at 863 (former CDK CEO Steve Anenen stating in a Q&A interview with *Dealer Magazine*: "There are a number of ways that third-parties have accessed data in the past with a dealer's permission, by doing a screen scrape or some other kind of access in order to get data. We won't prohibit that and we think dealers should be able to govern how they want that to happen."); Ex. 88, PX 1037 at CDK-00122549 (Dec. 2006) (CDK's Senior Vice President for Marketing telling *Automotive News*: "We don't tell the dealer, if someone wants access to their data, they have to come to [CDK] to gain access to the data. It's ultimately the dealer's data. If he wants to give that data to somebody, for us to try to charge a toll doesn't seem like the right thing to do. So we're not going to go down this path.");

[redacted]

Ex. 89, PX 1179 at CDK-0012546 ("That is the dealer's right. We have no right to tell them they can't do that"); [redacted]

[redacted] Ex. 150, Stejskal Rep. ¶ 77 ("CDK publicly took the position that the data in the DMS belonged to the dealers and that CDK would not interfere with companies that were providing integration services to dealers."); Ex. 9, Fitkin Reply Decl. ¶ 13, *Authenticom* Dkt. 141 ("For years, CDK took the position that the dealer owns that data and has the right to share that data with whomever it chooses.").

73. At least as far back as 2006, CDK sought to "clearly differentiate ADP's openness and security to the market by providing dealers with the most choices" for data integration. [redacted]; Ex. 84, PX 933 at CDK-0804066 (Feb. 19, 2007) (former CDK CEO Steve Anenen describing, in an interview with *Automotive News*, the "clear difference in philosophy" between CDK and Reynolds: "I don't know how you can ever make the opinion that the data is yours to govern and to preclude others from having access to it when in fact it's really the data belonging to the dealer. As long as they grant permission, how would you ever go against that wish? I don't understand that."); [redacted]

[redacted]; Ex. 150, Stejskal Rep. ¶ 77 ("CDK saw the data integration issue as an opportunity to differentiate itself from Reynolds. CDK publicly took the position that the data in

the DMS belonged to the dealers and that CDK would not interfere with companies that were providing data integration services to the dealers.").

74. [redacted]

75. In mid-2006, an industry coalition called Open Secure Access was formed to promote the principle that dealers should control who accessed their data, including through the use of dealer-authorized independent data integrators. Ex. 150, Stejskal Rep. ¶¶ 75-76 (describing the formation of the Open Secure Access coalition, including that "[t]hird parties that have dealer permission to utilize a dealer's data should be able to access the data through their own efforts or through the services of an independent company.")); Ex. 86, PX 1035 (press release announcing the formation of the Open Secure Access coalition on May 17, 2006).

76. In early 2007, CDK joined Open Secure Access. Ex. 131, CDK-3122862 at 863 (Mr. Anenen in *Dealer Magazine* interview: "As you know, ADP has joined the OSA (Open Secure Access) coalition. You can see our name now on its letterhead. We joined OSA for a couple of reasons. First and foremost, the principles that it has endorsed are exactly the same

principles that we hold near and dear to our own business philosophy: that dealership fundamentally owns the data in its DMS, and dealers should control who accesses their data and how it's used."); [redacted] Ex. 150, Stejskal Rep. ¶ 77 ("To more formally cement its position in the marketplace, CDK joined OSA just before an open letter to the industry was published in *Automotive News* in early 2007."); *see* Ex. 87, PX 1036.

77. Open Secure Access's guiding principles included (with "You" referring to dealers): "It's your data. *You* know best what to do with it." Ex. 87, PX 1036 ("We believe **DMS companies that support openness have the most to offer dealers**. Rather than use their leverage to reduce competition and increase dealer costs, these progressive DMS companies are actively contributing to facilitating innovation and increasing dealer profitability. Restrictive data policies have just the opposite effect *and* they hurt dealers."); *see* Ex. 150, Stejskal Rep. ¶ 77.

78. In 2009, Reynolds began implementing measures intended to make access by data integrators more difficult. Ex. 5, Cottrell Decl. ¶ 37, *Authenticom* Dkt. 62 ("Reynolds first started disabling Authenticom's polling services in 2009 when it introduced 'challenge questions' and 'captcha' (where the user has to enter random blurred text) to make it more difficult to automate the pulling of data."); [redacted]

79. From 2009 to 2013, Reynolds's technological measures were ineffective at preventing data integrators from accessing Reynolds's DMS. [redacted]

[redacted] Ex. 98, AUTH_00168635 (July 15, 2013) ("We have seen these lock out situations occur with Reynolds periodically – about 1X per year. These instances have caused a disruption in service and are an annoyance, but in all previous instances, we have been able to completely restore service for all dealers within a couple of weeks.").

80. [redacted] Mr. Witt was Vice President for Software Engineering and Development at DMI from 2006 to 2013.

81. Reynolds first began deploying simple "ASCII" CAPTCHA – which is CAPTCHA that was itself displayed as text characters on the screen – around 2010. Ex. 56, DX 1 at AUTH_00083637 (in May 2010, "R&R began prompting for ASCII Captcha"); Ex. 45, Brown Tr. 170:20-171:4 ("Reynolds originally released ASCII CAPTCHA."); [redacted]

82. Reynolds deployed graphical CAPTCHA – an image with distorted text – in or around 2013. Ex. 56, DX 1 at AUTH_00083637 (in May 2013, "R&R began prompting for Graphical Captcha").

83. In 2012, Reynolds began taking steps to disable login credentials that it suspected were being used by data integrators. Ex. 56, DX 1 at AUTH_00083637 (in February 2012, "R&R started disabling Report Generator profiles"); [redacted]

84. CDK and Reynolds disabled Authenticom's login credentials only after Authenticom used those credentials to access the DMS. Ex. 165, Declaration of Brian Clements (May 19, 2020) ("Clements 5/19/20 Decl.") ¶ 9**.**

85. The only successful method for responding to Reynolds's disabling of user credentials was for a dealer to re-enable existing credentials or to create new login credentials for Authenticom and other data integrators like DMI. Ex. 5, Cottrell Decl. ¶ 40, *Authenticom* Dkt. 62 ("After CDK and Reynolds disabled Authenticom's credentials, dealers worked cooperatively with Authenticom to set up new credentials and re-establish access. Given the sheer scale of the mass blocking, Authenticom was forced to redirect a majority of its 120-person workforce to the effort – including at one point hiring 50 temporary employees solely to help dealers navigate around the shutdowns."); Ex. 102, AUTH_00221965-66 (July 23, 2013) (Authenticom team working 12-hour shifts to call Reynolds dealers to re-enable blocked accounts); Ex. 99, AUTH_00169154 (Aug. 14, 2013) (Authenticom resolved more than 3,500 locked profiles by calling dealers between May 2013 and August 2013); [redacted]

86. Reynolds has advised dealers they can re-enable login credentials for their data integrators, when those connections are disabled. [redacted]

87. In August 2016, CDK for the first time implemented technological blocking measures that disabled the login credentials that dealers had created for data integrators. Ex. 5, Cottrell Decl. ¶ 39, *Authenticom* Dkt. 62 ("On August 1, 2016, CDK disabled Authenticom's login credentials, affecting thousands of dealership connections. Over the ensuing weeks and months, CDK repeatedly disabled Authenticom's login credentials for thousands of dealerships, severely disrupting the business operations of Authenticom's dealer and vendor clients."); [redacted]

88. [redacted]

89. [redacted].

90. [redacted]

91. Authenticom responded to Defendants' CAPTCHA by entering the text that was displayed on the screen; it has never bypassed a CAPTCHA without entering the correct response. Ex. 165, Clements 5/19/20 Decl. ¶ 14**;** Ex. 54, [redacted]

92. [redacted]

93. [redacted]

94. [redacted]

[redacted]

95. [redacted]

96. [redacted]

97. [redacted]

98. [redacted]

99. In mid-2016, CDK employed "Yes/No" prompts that presented users with the message that "The CDK Global DMS is for authorized Dealer personnel only. Use or access by unauthorized third parties is prohibited," prompting the user to "Enter 'YES' to confirm you are an authorized dealer employee in order to continue." [redacted]

100. [redacted]

101. It would take "a matter of minutes" for a programmer to modify software to respond "Yes" to the CDK "Yes/No" prompt. [redacted]

102. Within hours after first encountering CDK's "Yes/No" prompt, Authenticom modified its software to respond "Yes." Ex. 101, AUTH_00197254 at 259 (June 15, 2016, 12:38 PM) (Authenticom identifying the Yes/No prompt for the first time); Ex. 100, AUTH_00197253 (June 15, 2016, 8:03 PM) ("Zac pushed out an update for CDK polling to handle the authorization prompt that started today. The update is functioning and polling is working."); [redacted]

[redacted] Ex. 7, Gardner Decl. ¶¶ 63-64, *Authenticom* Dkt. 93 (noting CDK implemented the Yes/No prompts in 2016 and "[s]hortly after this prompt was implemented, Authenticom modified the hostile data extraction scripts it used to access the dealers' DMSs to answer this prompt 'YES'").

103. Authenticom always responded to the "Yes/No" prompts by answering "Yes"; Authenticom never attempted to go around the prompt without answering "Yes." Ex. 165, Clements 5/19/20 Decl. ¶ 15.

104. Authenticom developed a script called Profile Manager that dealers that use the CDK DMS could run to automate the process of re-enabling Authenticom's login credentials. Ex. 165, Clements 5/19/20 Decl. ¶¶ 4-6; Ex. 45, Brown Tr. 362:14-363:13 (Profile Manger is a "tool that was constructed to keep connections open" and works to "re-enable profiles that had been locked out."); Ex. 61, DX 817 at AUTH_00140426 (May 8, 2017) ("The sole purpose of the application is to repair usernames and passwords that you have previously setup and provided to your chosen service providers. These are the very same profiles that CDK has continually disabled, impacting the flow of your data to your vendors.").

105. The dealer runs Profile Manager from the dealer's computer system. Ex. 165, Clements 5/19/20 Decl. ¶ 7; Ex. 61, DX 817 at AUTH_00140426 (April 28, 2017) (Authenticom message to dealers regarding Profile Manager: "the Profile Manager tool provides you with BlueZone scripts to manage your vendor profiles," which allows "you to connect and run automated scripts on your DMS. The script initiated by the tool is not installed on the DMS; rather, it is run from a dealership PC and uses the DMS protocols in the same fashion a real user would use the system.").

106. Profile Manager uses tools built in to the CDK DMS that CDK makes available to the dealer to manage login credentials. Ex. 165, Clements 5/19/20 Decl. ¶ 5; Ex. 61, DX 817 at AUTH_00140426 (May 8, 2017) (with Profile Manager, the dealer runs a script from the dealer's PC and "uses the DMS protocols in the same fashion a real user would use the system.").

107. Dealers can run the Profile Manager program without enabling Authenticom's credentials. Ex. 165, Clements 5/19/20 Decl. ¶ 6.

108. Authenticom can access Defendants' "executable code" without encountering Defendants' technological measures, such as CAPTCHA, challenge prompts, and "Yes/No" prompts. Ex. 165, Clements 5/19/20 Decl. ¶ 13; Ex. 155, Miracle Rebuttal Rep. ¶¶ 21, 73-79.

109. CDK dealers are permitted to use software that dealers own or operate to provide "automated means" to export data from the DMS to third parties. Ex. 94, PX 1673 (January 9, 2020 letter from CDK's lead outside counsel, Britt M. Miller, stating that "any dealer validly licensing a CDK DMS that wishes to create and run reports and push data to a third party has the option to do so" and CDK will not block the dealer where "it is the *dealer* running the reports – either manually or using some form of automated means owned/operated by the dealer.").

110. In the computer security field, access controls determine what members of the organization or outside parties have permission to access certain data and to ensure that the data is made available only to those with sufficient authorization. Defendants' security expert conceded that their CAPTCHA did "not perform" this "authentication role." Ex. 161, IBM Computing Dictionary defining an "access control" as a "process" of "ensuring that the resource of a computer system can be accessed only by authorized users in authorized ways."); Ex. 160, (https://csrc.nist.gov/glossary/term/Access_control (glossary compiling definitions)); *e.g.*, *id.* (National Institute of Science and Technology defining access controls as the "[p]rocess of

granting access to information system resources only to authorized users, programs, processes, or other systems"); [redacted] Ex. 155, Miracle Rebuttal Rep. ¶ 13 ("In the field of software design and cybersecurity, a technological measure is considered to 'control access' if it requires a user to provide information (or perform some act) that is in the user's possession and indicates that the user has the computer or network administrator's authorization to obtain access."); Ex. 52, Tenaglia Tr. 197:17-20 (conceding that CDK and Reynolds's CAPTCHA did "not perform[ ] the authentication role,").

111. The DMS industry is a subset of the enterprise resource planning ("ERP") software industry. Ex. 157, Expert Rebuttal Report of Eric Kimberling ¶ 36 ("Dealerships predominantly use industry-specific ERP software known as Dealer Management Systems ('DMS')."") (citing documents from CDK and Reynolds describing the DMS as a type of ERP system).

112. ERP providers (such as Microsoft, Oracle, or SAP) do not prohibit their customers from hiring a software company to build a software interface for data integration. [redacted]

113. Authenticom has never had a data breach. Ex. 5, Cottrell Decl. ¶ 30, *Authenticom* Dkt. 62 ("Authenticom's security protections and protocol are state of the art. Authenticom has never had a data breach and its firewall has never been compromised."); Ex. 13, PI Hearing Tr. 1-A-114:12-14 (Q: "Has Authenticom ever had a data breach?" A: "Never once."). [redacted]

[redacted] Ex. 156, Expert Rebuttal Report of Peter Swire ¶ 94 ("As an initial matter, I note that Defendants' experts have presented no evidence that Authenticom (or other third-party Data Integrators) suffered a data breach.").

114. Reynolds has used Authenticom's data integration service for a variety of Reynolds's software applications, [redacted] Ex. 5, Cottrell Decl. ¶ 33, *Authenticom* Dkt. 62 ("Reynolds also uses Authenticom to pull data from a handful of Reynolds' own dealerships for use in Reynolds' own applications. Also, Reynolds uses Authenticom to pull data from non-CDK and non-Reynolds dealers for use in Reynolds' applications"); [redacted]

[redacted]

115. [redacted]

[redacted]

116. CDK has used Authenticom's data integration service for a variety of CDK applications, including AVRS, [redacted]

Ex. 3, Longpre Decl. ¶ 9 *Authenticom* Dkt. 55 (CDK dealer stating: "I also use a company called AVRS to provide electronic titling and vehicle registration services. AVRS uses Authenticom to pull my data off the DMS system."); [redacted]

117. Authenticom has never caused a data corruption problem on CDK's or Reynolds's DMS. [redacted]

[redacted]

118. Except for one incident in 2009 or 2010, Authenticom has never caused a system performance issue on Reynolds's DMS. [redacted]

119. In 2009 or 2010, there was a system performance problem on Reynolds's DMS attributable to Authenticom; Authenticom and Reynolds worked to resolve the issue within a single day. Ex. 10, Cottrell Reply Decl. ¶ 42, *Authenticom* Dkt. 143 (Authenticom CEO Steve Cottrell stating that, in 2009 or 2010, he "received a call from Reynolds's Vice President of OEM Relations and Data Services Robert Schaefer. He notified me of a malfunctioning system query and asked whether this could be an Authenticom query. I directed my team to investigate the issue; we found that the query did belong to Authenticom; and we corrected the problem the same day we were notified of it."); Ex. 12, PI Hearing Tr. 2-P-78 to 79 (Mr. Schaefer testifying with respect to the 2009 incident: "that's the only one I was specific on because it's the only one that I knew at a given point in time" to show Authenticom impairing DMS performance).

120. Mere access to a computer system – no matter how frequent – does not impair the performance of that computer system if there is unutilized computing power. Ex. 154, Expert Rebuttal Report of Adam Shostack ¶¶ 143-151.

Dated: May 20, 2020

Respectfully submitted,

/s/ Derek T. Ho

Derek T. Ho
KELLOGG, HANSEN, TODD, FIGEL & FREDERICK, P.L.L.C.
1615 M Street, NW, Suite 400
Washington, D.C. 20036
(202) 326-7900
dho@kellogghansen.com

Counsel for Authenticom, Inc.

CERTIFICATE OF SERVICE

I, Derek T. Ho, an attorney, hereby certify that on May 20, 2020 I caused a true and correct copy of the foregoing **PLAINTIFF AUTHENTICOM, INC.'S STATEMENT OF UNDISPUTED MATERIAL FACTS IN SUPPORT OF ITS MOTION FOR SUMMARY JUDGMENT ON DEFENDANTS' COUNTERCLAIMS** to be filed and served electronically via the Court's CM/ECF system. Notice of this filing will be sent by e-mail to all parties by operation of the court's electronic filing system or by mail to anyone unable to accept electronic filing as indicated on the Notice of Electronic Filing. Parties may access this filing through the Court's CM/ECF system. Copies of the Under Seal filing were served on counsel of record via email. Copies of the Under Seal filing were served on counsel of record via email.

/s/ Derek T. Ho

Derek T. Ho
KELLOGG, HANSEN, TODD, FIGEL & FREDERICK, P.L.L.C.
1615 M Street, NW, Suite 400
Washington, D.C. 20036
(202) 326-7900
dho@kellogghansen.com